DirectTrust

Building the Security and Trust Framework for Direct Exchange

North Dakota Health IT Summit

Brian Ahier

Brian.Ahier@DirectTrust.org

Mission and Goals: DirectTrust

DirectTrust.org, Inc. (DirectTrust) is a voluntary, self-governing, non-profit trade alliance dedicated to the support of Direct exchange of health information, and to the growth of Direct exchange at national scale, through the establishment of policies, interoperability requirements, and business practice requirements that will enhance public confidence in privacy, security, and trust in identity. The latter, taken together, create a Security and Trust Framework for the purpose of bridging multiple communities of trust.

DirectTrust is the recipient of an ONC Cooperative Agreement award in the amount of $280,205 as part of the Exemplar HIE Governance Program. Within this Program, DirectTrust is charged by ONC with further development of the Direct Trusted Agent Accreditation Program, and the build out of a national trust anchor bundle distribution service for Direct exchange.

DirectTrust Priority Goals Under the EHIEGE Program

- ✓ Increase interoperability, decrease cost and complexity, and facilitate trust among participants using Direct for health information exchange of personal health information for health care improvements.

- ✓ Advance industry engagement in the Electronic Healthcare Network Accreditation Commission (EHNAC)-DirectTrust program for voluntary accreditation of HISPs, CAs, and RAs, who act as trusted agents on behalf of Direct exchange participants (DTAAP).

- ✓ Design, build out, and operate at scale a Trust Anchor Bundle Distribution Service, TABs, that transparently identifies attributes of anchor certificates from accredited HISPs, and distributes these anchors to the public, thereby permitting trust relationships to grow at "scale," and removes the need for costly, time consuming, one-off contract negotiations between HISPs or their users/subscribers.

Mission and Goals: EHNAC

Founded in 1993, the Electronic Healthcare Network Accreditation Commission, EHNAC, is a federally-recognized standards development organization and tax-exempt 501(c)(6) non-profit accrediting body designed to improve transactional quality, operational efficiency, and data security in healthcare.
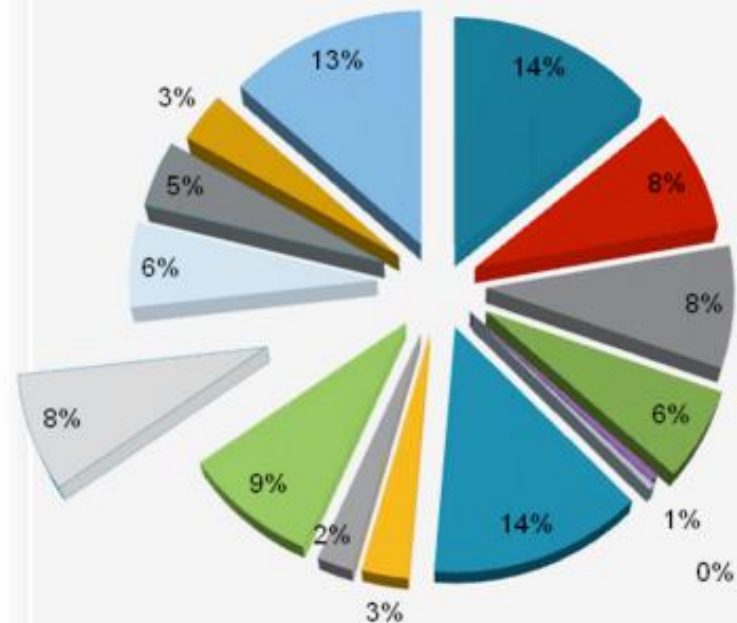
DirectTrust and EHNAC have formed a partnership to accredit trusted agents in Direct, HISPs, Certificate Authorities, and Registration Authorities, in order to facilitate security and trust at scale, helping to avoid the need for costly and complicated one-off contractual arrangements between relaying parties in Direct exchange.

The problem Direct exchange is designed to help solve - fragmentation

DirectTrust — Collaborating to Build the Security and Trust Framework for Directed Exchange

Example of HIT Fragmentation in One County (actual data) near Phoenix, Az.

- **6400+** physicians using **70+** EHR vendors

- **58** of these vendors representing fewer than 100 physicians each

- **8%** of this county's physicians using Epic (2 IDNs)

- **104+** Walgreens and **64+** CVS pharmacies**

- **8 HIEs** and the Immunization Information System (IIS) State Registry

- **Diagnostic imaging** centers, **lab** information systems, and **long term care** providers

Estimated Number of Physicians by EHR Vendor in Example County*

14%, 13%, 3%, 5%, 6%, 8%, 9%, 2%, 3%, 14%, 0%, 1%, 6%, 8%, 8%

DirectTrust

Collaborating to Build the Security and Trust Framework for Directed Exchange

- Direct exchange is well suited to replace fax, e-fax, mail, and proprietary connections:
  - Between providers during transitions of care;
  - Between providers and patients;
  - Between federal and state agencies and providers for document exchange, requests for information;
  - Between payers and provider organizations;
  - Between patients and patient applications for organization, display, reconciliation, analysis.

HISP definition

1. In order for there to be Direct services, there must be a Health Information Service Provider, HISP.

2. A HISP is an entity that conducts the secure transmission of Direct messages to and from Direct Addresses, each of which is bound to a Direct X.509 digital certificate (i.e. provides "Direct Services").

3. A HISP may act in the capacity of a Business Associate or Contractor for the Customer, in which case the HISP may hold and manage PKI private keys associated with Direct digital certificates on behalf of the Customer's users/addressees.

4. A HISP may be a part of a larger organization that offers and performs services that are beyond the boundary of the HISP's roles and responsibilities.

5. A HISP does NOT use, manage, analyze, or otherwise perform actions upon the information transmitted and made secure.

DirectTrust is an outgrowth of the Direct Project "Rules of the Road" WG

DirectTrust
Collaborating to Build the Security and Trust Framework for Directed Exchange

X.509 Certificate Policy Established
December 2011

→

Accreditation Program Kick-off
February 2013

→

ONC Cooperative Agreement Award
March 2013

→

Trust Anchor Bundle Distribution Service Started
May 2013

- DirectTrust's membership includes over 80 entities, including state HIEs and state agencies, coalitions, HISPs, EHR vendors, provider groups, certificate authorities, consultants, and private individuals.

- DirectTrust members are serving Direct users/subscribers in all 50 states as HISPs, CAs, and RAs within the context of Stage 2 Meaningful Use, and beyond.

- DirectTrust is the only national Security and Trust Framework provider for Direct, and in partnership with EHNAC, the sole accrediting body for Direct trusted agents – HISPs, CAs, and RAs.

How it works: Single HISP exchange is Email via an encrypted session

ARC OF LIABILITY

Recipient

Web portal
Receiving System — SSL/TLS — HISP A

Endpoint Communication
(XDR, SMTP, others)

Recipient

SMTP Server

Receiving System — SSL/TLS

Outlook

SSL/TLS

SSL/TLS

HISP A subscribers

Sending System

EHR

Sender

Sending System — MacMail

Sender
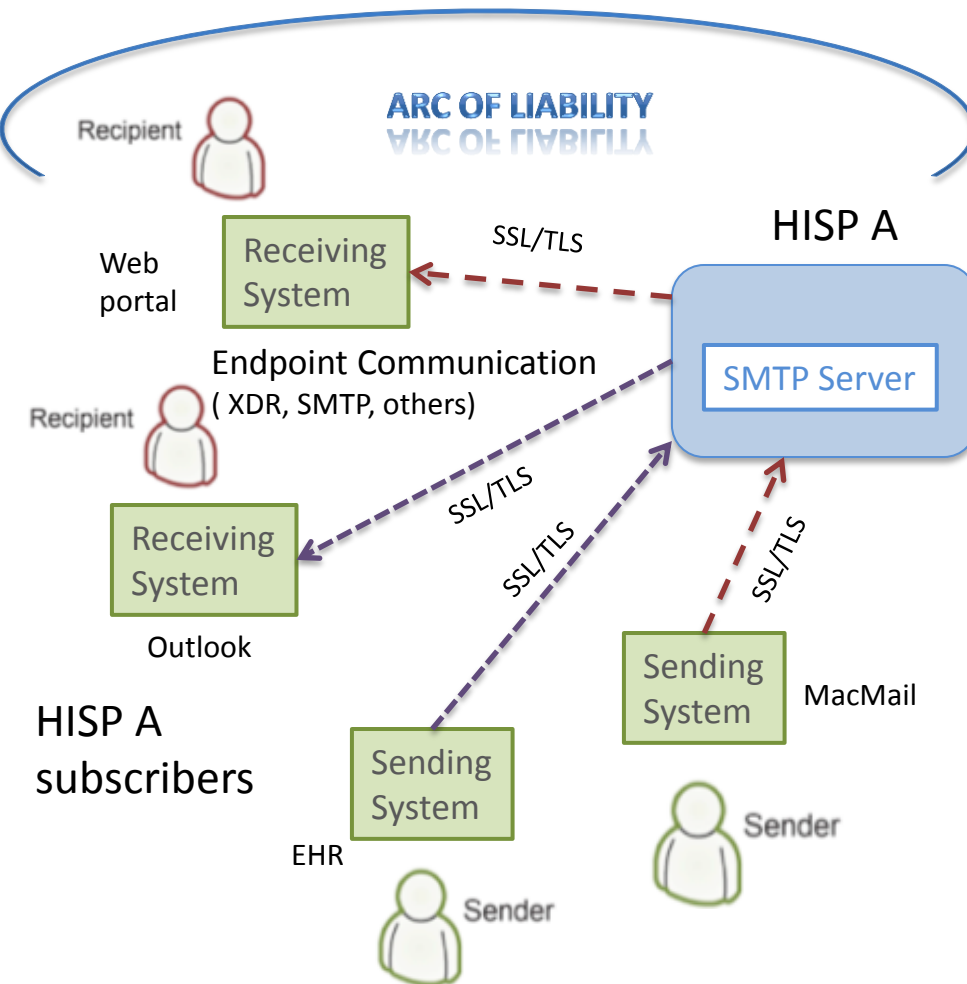
Central hub for all HISP's subscribers.
Direct STA not invoked.
No use of Direct certificates.
At this point, exchange is limited
to subscribers of this HISP.

HISP-HISP Direct exchange adds in a layer of security & trust in order to enable *point-to-point* exchange between subscribers of *different* HISPs, over the Internet, *without* a central hub.

DirectTrust Collaborating to Build the Security and Trust Framework for Directed Exchange

ARC OF LIABILITY

Sending HISP

Security/Trust Agent

SMTP Server

Receiving HISP

Security/Trust Agent

SMTP Server

identity validation

Direct (SMTP / SMIME)

encryption

MaxMD

careaccord™ Oregon's Health Information Exchange

SSL/TLS

Endpoint Communication (XDR, SMTP, others)

Endpoint Communication (XDR, SMTP, others)

SSL/TLS

MacMail

Sending System

Web portal

Receiving System

Sender

Recipient

dkibbemd@direct.kibbe.md

DrSusan@direct.cardiology.com

HISP-HISP between EHRs

HISP-HISP exchange between EHR and PHR
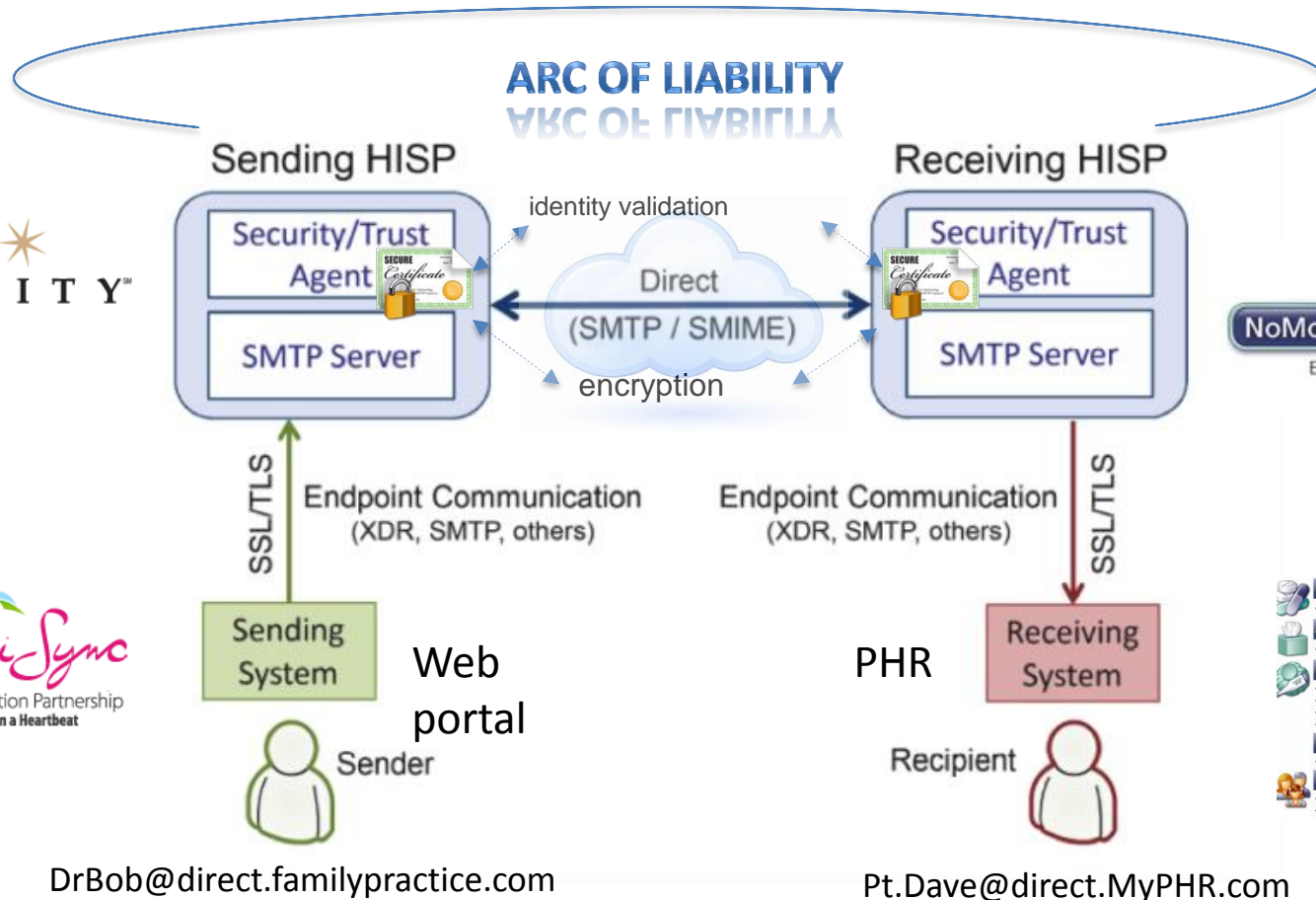
Questions to resolve

- How does HISP A know that HISP B…X,Y,Z are trustworthy enough to exchange HISP's subscribers' Personal Health Information with them? What are the risks?

- How does HISP A establish a baseline of assurance regarding security and trust-in-identity with HISP B…X,Y,Z ?   A baseline that will scale?

- What mechanisms are available for HISP A to signal its trustworthiness to others, efficiently and at scale?

Building a Network via Bi-directional Contracts is Unworkable

- If HISPs choose to negotiate the "rules of the road" with each other one at a time, forging one-off contracts, the cost of Directed exchange *goes up* with each new HISP contract. Complex. Rate limiting. Will not scale.

Scalable Trust and the N-squared problem

- Scalable Trust is a strategy for enabling Directed exchange between a large number of endpoints, in this case HISPs and their users/subscribers.

- If "scalable,"
  - Trust should happen "quickly" and uniformly.
  - A "complete" network will be formed voluntarily.
  - Complexity and cost of establishing a network will decrease, while the value of the network itself will increase, as more nodes are added.
  - This "network effect" will be a by-product of making trust scalable.
  - Eliminates the need for one-off manual business agreements and technical connection.s

- If not "scalable,"
  - Parties will be forced to create one-off manual business agreements and technical connections increasing cost and complexity.
  - Manual exchange and maintenance of trust anchors doesn't scale beyond the smallest of numbers – N-squared problem.
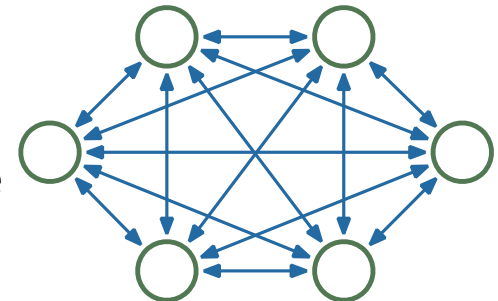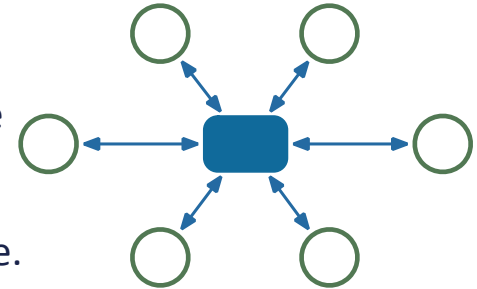
DirectTrust Approach

The goal is to make it easy and inexpensive for trusted agents, e.g. HISPs, to voluntarily know of and follow the "rules of the Road," while also easily and inexpensively knowing who else is following them.

Security & Trust Framework

EHNAC-DirectTrust Accreditation Program

Trusted Anchor Bundle Distribution

DirectTrust Approach

Avoid this:

> **The site's security certificate is not trusted!**
>
> You attempted to reach **1.1.1.1**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.
>
> You should not proceed, **especially** if you have never seen this warning before for this site.
>
> [Proceed anyway]   [Back to safety]
>
> ▶Help me understand

With this:

DirectTrust / EHNAC / ACCREDITED DTAAP HISP

DirectTrust / EHNAC / ACCREDITED DTAAP CA

DirectTrust / EHNAC / ACCREDITED DTAAP RA

Separate roles and responsibilities for "trusted agents" to the exchanges determine separate accreditation tracks

DirectTrust — Collaborating to Build the Security and Trust Framework for Directed Exchange

Healthcare Organization (HCO)

HCO Direct Addressees

The HCO relies on HISP, CA, and RA as accredited trusted agents, and bears ultimate responsibility for HIPAA privacy and security.

Basic services for user: DNS discovery; encryption; certificate signing and validation; send/receive MDNs; provide HISP-side of edge protocol connection compliance with Direct standard,

Health Information Service Provider (HISP)

The HISP enforces the policies specified in the DirectTrust HISP Policy (HP), and MUST use accredited RA and CA.

Registration Authority (RA)

Compile/Validate Identity and Trust Documentation

The CA and RA enforce the policies specified in the DirectTrust and FBCA Certificate Policy (CP).

Certificate Authority (CA)

| X.509 Certificate Issuance Service | Certificate Validation Service |
| Certificate Signing Services | Revocation Services |

Identity vetting at a specific level of Assurance, LoA.

Registration Authority

Credential issued on the basis of RA's Identity vetting at specific LoA..

Certificate Authority

www.DirectTrust.org
1101 Connecticut Ave NW, Washington, DC 20036

18

Trusted agents: key roles and responsibilities for HISPs, CAs, RAs

Relying Parties

Trusted Agents

Healthcare Organizations/Providers/Patients/Consumers

HISP
Provides accounts and addresses to Direct users, performs STA functions of encryption, signing of messages, DNS discovery, etc. Relies on CA, RA policies and practices. Adheres to DirectTrust HISP Policy.

Certificate Authority
Issues Direct X.509 digital certificate to unique Direct address, relying on RA's policies and practices, and at the corresponding LoA(s). Manages certificates, e.g. revocation services, certificate validation services. Adheres to DirectTrust Certificate Policy.

Registration Authority
Provides identity proofing and verification relying on trusted documents at known levels of assurance, LoA. Securely passes that information to Certificate Authority. Updates identity Information as required. Adheres to policies for identity verification in DirectTrust Certificate Policy, based upon NIST 800-63-1, FICAM, FBCA CP.

Criteria: Programs and Sections

- 3 Programs: DTAAP-HISP, DTAAP-CA, and DTAAP-RA
- The first five criteria sections in each are identical (75 criteria):
  - I. Introduction to Candidate Environment
  - II. Privacy and Confidentiality
  - III. Technical Performance
  - IV. Resources
  - V. Security
- Section VI is unique to each program:
  - HISP (14 criteria), CA (64 criteria), or RA (56 criteria)

www.DirectTrust.org
1101 Connecticut Ave NW, Washington, DC 20036

EHNAC Accreditation Process

Pre-application
- Ensures qualification based on type of business

Application
- Collects additional information and annual fees

Self-Assessment
- Demonstrates evidence of compliance with criteria

Site Review
- Tests Self-Assessment claims via on-site review.

Award
- Awards level of accreditation achieved (Full, Provisional, Interim, Failed).

Timeline
Candidate is approved and has 1 year to complete. Maximum 8 mos. to submit the self-assessment allowing up to 4 mos. for site review(s), final report and approval process

www.DirectTrust.org
1101 Connecticut Ave NW, Washington, DC 20036

Trust anchor bundles

HISP Accreditation via EHNAC-DirectTrust

- HISPs apply for accreditation, become candidates for DTAAP HISP
- HISPs complete self-attestation and audit, successful complete accreditation

HISP obtains trust anchor from accredited CA in accordance with DirectTrust Standard Operating Policies document.

HISP submits its trust anchor to DirectTrust Review Committee.

Upon successful review, HISP's trust anchor is included in trust anchor bundle, available on EV cert-protected website, Bundles.DirectTrust.org .

HISPs may upload bundle of trust anchors, and place trust anchors in their HISP trust stores, readying themselves to trust incoming request from subscribers of these accredited HISPs using end-entity certificates that march anchors.

Packaging & Distribution
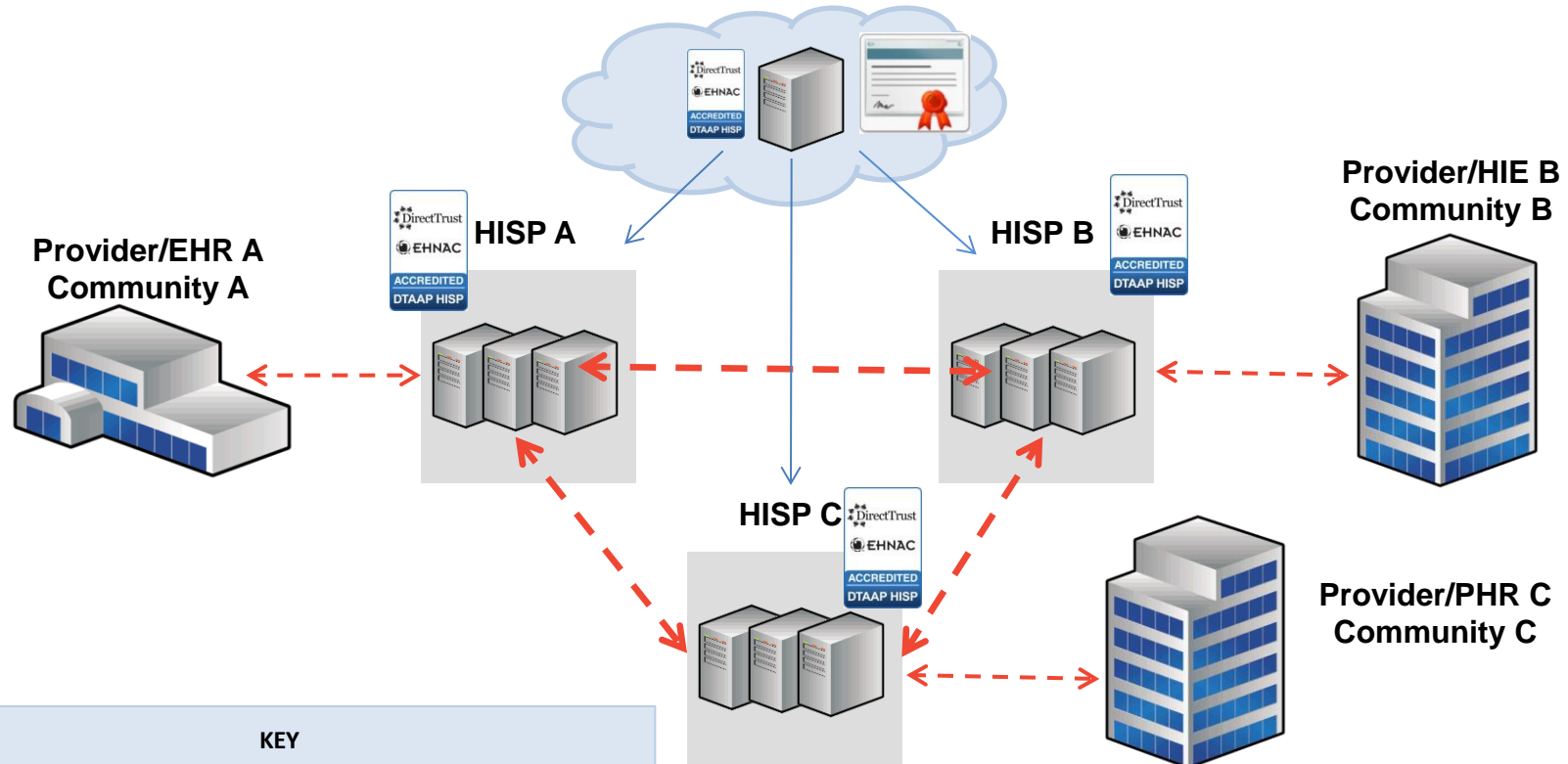
Trust Community Anchor Distribution Site

Bundle(PKCS7)

HTTP(S)

HISP — Trust Store

HISP — Trust Store

HISP — Trust Store

HISP — Trust Store
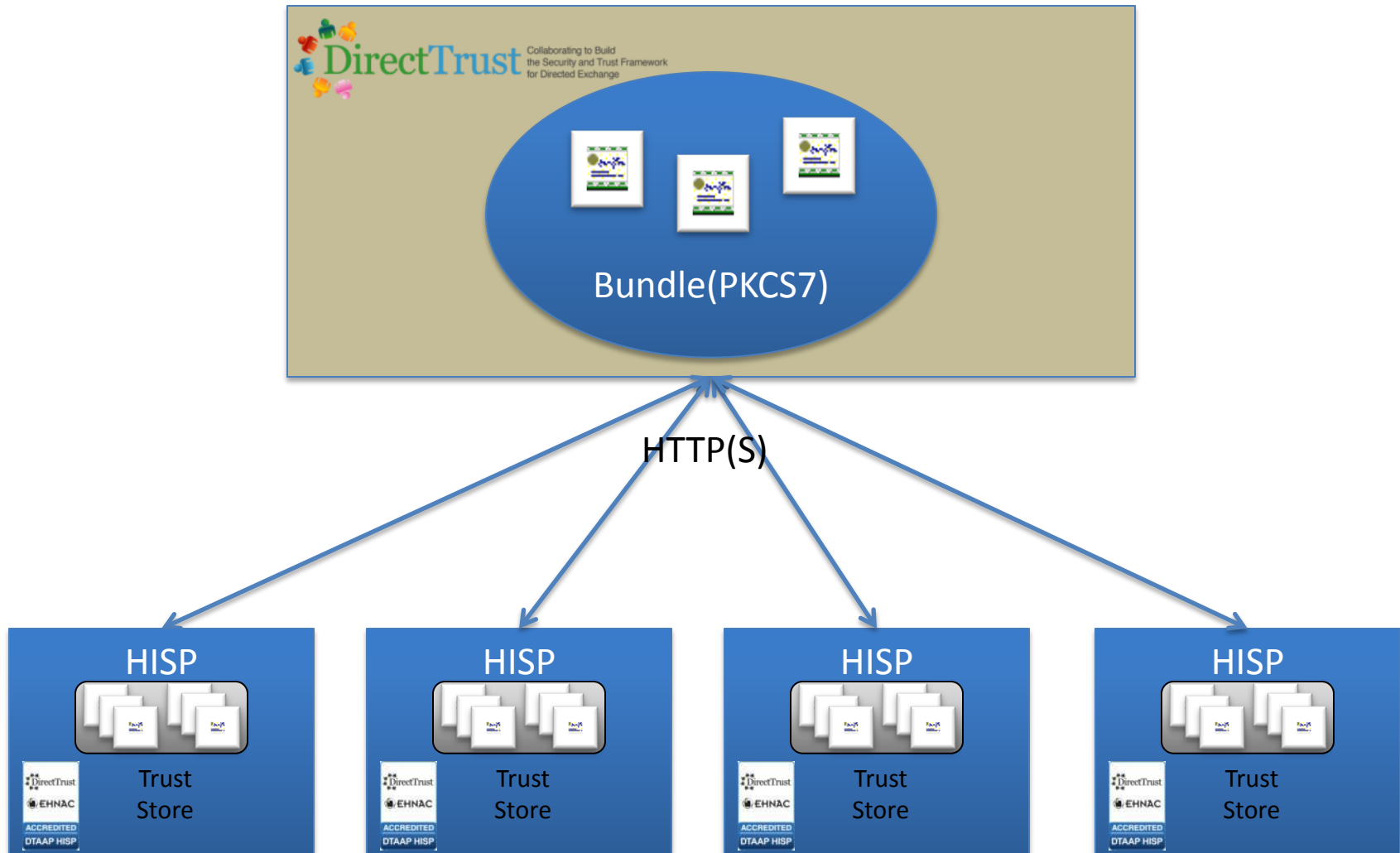
Example of the DirectTrust Community's "Scalable" Trust

Centralized Trust Anchor Bundle Site

Provider/EHR A Community A

HISP A

HISP B

Provider/HIE B Community B

HISP C

Provider/PHR C Community C

KEY

- - - - Trust relationship based on accreditation

Resources and additional information

- DirectTrust website www.DirectTrust.org

  Information on Membership
  Information on Workgroups and Active Projects
  DirectTrust Membership List
  Accreditation Status List
  Code of Ethics
  DirectTrust Community X.509 Digital Certificate Policy
  Federation Agreement
  Direct Trusted Agent Accreditation Program (DTAAP)
  Trust Anchor Bundle Website

  Brian.Ahier@DirectTrust.org